

CLAIMS

1 A method for analyzing a logfile produced by a computer network security system, comprising:

providing a regular expression query associated with a pattern to be
5 searched for in the logfile; and

using the query to search for the pattern in the logfile.

2. The method as recited in claim 1, wherein the pattern is associated with a possible
10 *sgid* exploit.

3. The method as recited in claim 2, wherein using the query to search for the pattern
includes searching for entries showing that a process has been started with effective
group ID equal to zero.

15 4. The method as recited in claim 3, wherein using the query to search for the pattern
further includes storing a process ID of the process, and searching for processes with a
parent process ID equal to the stored process ID.

5. The method as recited in claim 1, wherein the pattern is associated with a possible
20 *suid* exploit.

6. The method as recited in claim 5, wherein using the query to search for the pattern includes searching for entries showing that a process has been started with effective user ID equal to zero.

5 7. The method as recited in claim 6, wherein using the query to search for the pattern further includes storing a process ID of the process, and searching for processes with a parent process ID equal to the stored process ID.

8. The method as recited in claim 2, wherein the pattern is associated with processes spawned by a shell.

9. The method as recited in claim 8, wherein using the query to search for the pattern includes searching for entries showing that the shell has started a process, storing a process ID of the process, and searching for entries showing processes with parent process ID equal to the stored process ID.

10. The method as recited in claim 2, wherein the pattern is associated with user keystrokes, and the method further comprises aggregating the user keystrokes found in the logfile.

11. The method as recited in claim 10, wherein the found user keystrokes are aggregated upon finding a keystroke representing a newline character.

12. The method as recited in claim 11, further comprising presenting the aggregated keystrokes to a second user.

13. The method as recited in claim 2, wherein the pattern is associated with screen
5 output characters, and the method further comprises aggregating the screen output characters found in the logfile.

14. The method as recited in claim 13, wherein the found screen output characters are aggregated upon finding a screen output character representing a newline character.

15. The method as recited in claim 14, further comprising presenting the aggregated keystrokes to a second user.

16. The method as recited in claim 1, wherein the pattern is associated with files to be
15 monitored.

17. The method as recited in claim 2, wherein using the query to search for the pattern includes searching for entries showing that a monitored file has been accessed.

20 18. The method as recited in claim 17, further comprising indicating to a second user a filename of the accessed monitored file.

19. The method as recited in claim 17, further comprising indicating to a second user a process ID of a process that accessed the monitored file.

20. The method as recited in claim 19, further comprising automatically searching for the process ID in the logfile.

21. The method as recited in claim 2, wherein using the query to search for the pattern includes searching for entries showing that an attempt has been made to access a monitored file.

22. A method for providing security for a computer network, comprising:

- generating content sets for a computer associated with the network;
- determining whether a user should be routed to the generated content sets;
- selecting one of the content sets if it is determined that the user should be routed to the generated content sets;
- routing the user to the selected generated content set;
- producing a logfile of at least a portion of the user's activity with respect to the computer; and
- using at least one regular expression query to analyze the logfile.

23. The method as recited in claim 22, further comprising associating each generated content set with a virtual computer.

24. The method as recited in claim 23, wherein selecting one of the content sets includes choosing a content set associated with a virtual computer requested to be accessed by the user.

5 25. The method as recited in claim 24, wherein producing the logfile includes storing information regarding the user's activity with respect to the selected content set and associated virtual computer.

26. The method as recited in claim 25, wherein the computer is running on a Solaris
10 operating system.

27. A system for analyzing a logfile produced by a computer network security system, comprising:

15 a storage including a regular expression query associated with a pattern to be searched for in the logfile; and

a processor configured to use the query to search for the pattern in the logfile.

28. The system as recited in claim 27, wherein the pattern is associated with a
20 possible *sgid* exploit.

29. The system as recited in claim 28, wherein the processor is further configured to search for entries showing that a process has been started with effective group ID equal to zero.

5 30. The system as recited in claim 29, wherein the processor is further configured to store a process ID of the process, and search for processes with a parent process ID equal to the stored process ID.

31. The system as recited in claim 27, wherein the pattern is associated with a possible *suid* exploit.

32. The system as recited in claim 31, wherein the processor is further configured to search for entries showing that a process has been started with effective user ID equal to zero.

33. The system as recited in claim 32, wherein the processor is further configured to store a process ID of the process, and search for processes with a parent process ID equal to the stored process ID.

20 34. A system for providing security for a computer network, comprising:
a computer configured to generate content for the computer, wherein the computer is associated with the network;

a network device configured to determine whether a user should be routed to the generated content and to route the user to the generated content if it is determined that the user should be routed to the generated content;

a logging mechanism configured to produce a logfile of at least a portion of the user's activities with respect to the generated content; and

a storage including a regular expression query usable by the computer to search the logfile for a pattern associated with the regular expression query.

35. A computer program product for analyzing a logfile produced by a computer network security system, comprising a computer usable medium having machine readable code embodied therein for

providing a regular expression query associated with a pattern to be searched for in the logfile; and

using the query to search for the pattern in the logfile.

36. A computer program product for providing security for a computer network, comprising a computer usable medium having machine readable code embodied therein for

generating content sets for a computer associated with the network;

determining whether a user should be routed to the generated content sets;

selecting one of the content sets if it is determined that the user should be routed to the generated content sets;

routing the user to the selected generated content set;

d

producing a logfile of at least a portion of the user's activity with respect to the computer; and

using at least one regular expression query to analyze the logfile.

09241639 042301